UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
WESTERN DIVISION

LINDSEY WILLIAMS-DIGGINS, individually and on behalf of all others similarly situated, *Plaintiff*, *v.* MERCY HEALTH, an Ohio non-profit corporation, *Defendant*.	Case No.: 3:16-cv-1938 **JURY DEMAND** Hon. Jeffrey J. Helmick

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiff Lindsey Williams-Diggins brings this First Amended Class Action Complaint ("Complaint") against Defendant Mercy Health ("Mercy" or "Defendant") to obtain relief from Defendant's failure to protect patients' private medical information with promised data security. Plaintiff alleges as follows upon personal knowledge as to himself and his own acts and experiences, and upon information and belief, including investigation conducted by his attorneys, as to all other matters.

NATURE OF ACTION

1. Defendant Mercy is the largest health system in the State of Ohio, with 23 hospitals, dozens of smaller facilities, and over 1,000 physicians located through the state. In 2015 alone, Mercy generated over $4 *billion* in revenue. As a part of its services, Mercy creates, operates, and maintains websites where employees and patients can access patients' medical data online.

2. Unfortunately, Defendant failed to keep its patients' sensitive medical information secure. On August 2, 2016, Plaintiff filed a class action complaint alleging that Defendant's computer systems suffered from a critical vulnerability in three of its internet and publicly accessible websites. The result of the vulnerability was that private medical information entrusted to Mercy by its patients had been exposed and was at great risk of further unauthorized disclosure and breach (if it hadn't already been breached).

3. According to Plaintiff's expert, this "critical vulnerability exploit" was known to those in the cyber security industry since at least 2013 and could have been "mitigated relatively quickly and cheaply without incurring unreasonable costs."[1] Despite this cheap fix, Plaintiff alleged that Mercy eschewed security and exposed patient data. In fact, it was possible that "once an attacker control[ed] [Mercy's] server, the attacker [could have] obtain[ed] connection information regarding other computer or devices" on Mercy's networking, resulting in the attacker having "unfettered access to Mercy Health's internal computer network, data stores, and possibly, network connected medical devices."

4. Plaintiff alerted Mercy about the vulnerability by filing his Complaint, which

[1] Expert Declaration of Craig J. Snead ("Snead Decl.") at ¶¶ 9, 16. A true and accurate copy of the Snead Declaration is attached hereto as Exhibit A.

Mercy repaired a few days later (i.e., on August 5, 2016). While this fix stands to better protect Plaintiff's and other Class Members' patient data moving forward, it cannot turn back the clock and correct months—if not years—of Mercy's continual and demonstrated failure to protect the patient data entrusted to it. In fact, because of this extended, easily exploitable, and unmitigated exposure of patient data, Mercy's patients remain at risk of suffering further harm from the long-term exposure of their confidential and sensitive information (i.e., until a third party is able to confirm that—despite Mercy's lackluster data practices—patient data was not compromised during that time period).

5. Beyond the palpable risk created by its actions, by exposing Plaintiff and the putative Class's private medical information for months or even years, Mercy additionally injured its patients by charging and collecting market-rate medical fees without providing industry standard protections for patient data confidentiality. Worse, by choosing to operate its public websites with critical—and well-known—vulnerabilities, like the one identified by Plaintiff, Defendant failed (and, in all likelihood, continues to fail) to adequately allocate resources necessary to maintain patient data security.

6. Accordingly, this putative class action lawsuit seeks, among other things, (i) damages and restitution, (ii) to compel Mercy to allow an independent, third-party firm to conduct a security audit, (iii) to inform patients with information stored by Mercy that their information was exposed, and (iv) attorneys' fees and costs.

PARTIES

7. Plaintiff Lindsey Williams-Diggins is a natural person and citizen of the State of Ohio.

8. Defendant Mercy Health is a non-profit corporation incorporated under the laws

of the state of Ohio with a principal place of business at 1701 Mercy Health Place, Cincinnati, Ohio 45237. Defendant conducts business throughout this District, the State of Ohio, and the United States.

JURISDICTION AND VENUE

9. Federal subject-matter jurisdiction exists under 28 U.S.C. § 1332(d)(2) because (a) at least one member of the class is a citizen of a state different from Defendant, (b) the amount in controversy exceeds $5,000,000, exclusive of interests and costs, and (c) none of the exceptions under that subsection apply to this action.

10. The Court has personal jurisdiction over Defendant because Defendant is registered to conduct business in the State of Ohio, conducts significant business transactions in this District, and because the wrongful conduct occurred in and/or was directed to this District.

11. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to Plaintiff's claims occurred in this District, Plaintiff resides in this District, and because Defendant resides in this District.

FACTUAL ALLEGATIONS

I. Mercy Has a Duty to Secure Patients' Data in its Portals.

12. Mercy is the largest health system in the State of Ohio. Mercy employs over 1,000 physicians and 32,000 others in its network of 23 hospitals and dozens of clinics and facilities. Mercy operates in Ohio and Kentucky. Mercy generates more than $4 billion of revenue per year and services hundreds of thousands of patients.

13. For each patient, Mercy creates and maintains detailed records of health status and the treatments provided. While some of these records exist in paper format, Mercy maintains electronic copies of patient medical records and stores those records in its computer systems.

These systems are further connected to the internet and act as portals into Mercy's patient data repositories.

14. One such system Mercy has implemented is the Horizon Patient Folder WebStation portal (the "WebStation"), created by non-party McKesson Corporation. McKesson describes the WebStation as a "document management and imaging solution that electronically captures, indexes, completes and stores a legal electronic medical record" and that allows for "[e]asy access to patient information."[2] Mercy's WebStation is publicly available at the addresses: 168-250-52-64.health-partners.org, 168-250-52-65.health-partners.org, and 168-250-52-66.health-partners.org.

15. On these websites, Mercy maintains its patients' private medical information in electronic storage. As such, Mercy is a covered entity under the Healthcare Insurance Portability and Accountability Act ("HIPAA"), which regulates the privacy of patient information.[3] And, Mercy must comply with HIPAA regulations.

16. Moreover, Mercy regularly receives, maintains, and transmits Protected Health Information, which HIPAA defines as information that is transmitted or maintained in any form or medium, including:

> a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.[4]

[2] *OneContent Patient Folder | McKesson*, http://www.mckesson.com/providers/health-systems/diagnostic-imaging/enterprise-document-management-system/onecontent-patient-folder/ (last visited Sept. 6, 2016).

[3] 45 C.F.R. § 160.103.

[4] *Id*.

17. Based on obligations created by HIPAA, industry standards, and promises it made to its patients, Mercy had an obligation to keep its patients’ private medical information confidential and protect the information from exposure and unauthorized disclosure. Class members provided their private medical information to Mercy with the understanding that Mercy would comply with its duty and obligations to keep the information confidential and secure from exposure and further unauthorized disclosures.

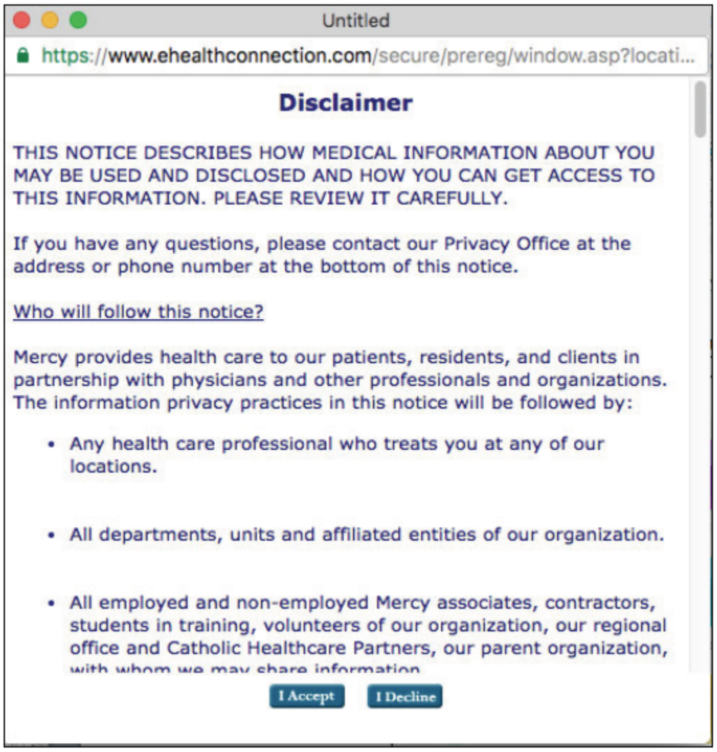
18. Mercy admitted its duty to keep patients’ medical information confidential and secure through its own statements. Through its Notice of Privacy Practices (which all patients receive), Mercy promised to keep patients’ medical information confidential and protect it from exposure and unauthorized disclosure. For instance, the Notice of Privacy Practices states, in relevant part:[5]

> **Our Pledge to You**
> We know your medical information is personal and we are committed to protect your privacy. We create a record of your care and services to meet legal requirements and to provide you the best care. This notice applies to your medical record that we maintain for services or items we provide you at our locations. Your personal doctor may follow a different notice for your medical record created and maintained in his or her office. We are required by law:
>
> - To keep medical information about you private.
> - To give you this notice, explaining our legal duties to protect your privacy.
> - To follow the terms of the notice that is currently in effect.
> - To notify you if we fail to protect your privacy.
>
> …
>
> In following privacy laws and regulations, we must meet the stricter of state or federal laws and regulations. Where state laws are stricter than federal laws, we will meet the applicable state law.
>
> …

[5] A true and accurate copy of Defendant’s Notice of Privacy Practices is attached hereto as Exhibit B.

> We may share your medical information with business associates that contract with this health system. All business associates must follow this notice, and are directly responsible for compliance with applicable state and federal privacy laws and regulations.
>
> **Authorizations and other uses of medical information**
> In any other situation not covered by this notice, we will ask for your written permission before sharing your medical information. For example, your permission is required to release your information for most research or marketing, to sell your medical information, or to share your psychotherapy notes. If you provide written permission to release your information, you can later notify us in writing to cancel your permission.

19. Mercy requires each patient to accept the terms of its Notice of Privacy Practice and acknowledge receipt of the terms prior to obtaining care. For instance, Mercy requires patients who seek to pre-register online to "Accept" or "Decline" the terms of the Notice of Privacy Practices before registration can occur:


Untitled
https://www.ehealthconnection.com/secure/prereg/window.asp?locati...
I Accept
I Decline

Disclaimer

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

If you have any questions, please contact our Privacy Office at the address or phone number at the bottom of this notice.

Who will follow this notice?

Mercy provides health care to our patients, residents, and clients in partnership with physicians and other professionals and organizations. The information privacy practices in this notice will be followed by:

- Any health care professional who treats you at any of our locations.
- All departments, units and affiliated entities of our organization.
- All employed and non-employed Mercy associates, contractors, students in training, volunteers of our organization, our regional office and Catholic Healthcare Partners, our parent organization, with whom we may share information

(**Figure 1**.)

20. Mercy recognized the importance of keeping patients' private medical information confidential and further promises to protect that information and comply with data

security requirements mandated by, among other things, federal and state privacy laws. For instance, in its Corporate Responsibility statement, Mercy states the following:

> Associates throughout Mercy Health also receive special training in the federal HIPAA (Health Insurance Portability and Accountability Act) regulations that protect the privacy and security of patient health information, and they are held accountable for abiding by them. In compliance with HIPAA, all patients of Mercy Health facilities receive a copy of the facility's Notice of Privacy Practices.[6]

21. And in its "Core Values" document, Mercy states that:

> Our associates keep patient information confidential, obeying the laws and rules that apply, including HIPAA and more stringent state laws. They prevent the release of any personal or confidential information about a patient unless it is needed for lawful business or patient care. They also do not seek personal or private information about any patient if they do not need it to complete their duties.[7]

22. And only one month prior to the filing of Plaintiff's original complaint, Defendant issued a "news release" naming "Mercy Health a 2016 Most Wired Healthcare System" in an effort to market itself as a technologically advanced and secure hospital. In that release, Mercy publicized:

> "At Mercy Health, technology helps us drive both greater access and better care for our patients," said Rebecca Sykes, Mercy Health Chief Information Officer. "Enhancements to our electronic medical record system will enable us to offer e-visits widely and share more information with our patients to help them partner with our providers in their care."
>
> …
>
> As they build out new capabilities, hospitals are also taking strong actions to ensure health data is secure.
>
> - More than 90 percent use intrusion detection systems, privacy audit systems

[6] *Corporate Responsibility | Mercy Health Corporate*, www.mercy.com/corporate/corporate-responsibility.aspx (last visited Sept. 6, 2016).

[7] *Corporate Responsibility: Core Values In Action*, http://www.mercy.com/corporate/pdfs/CoreValues.pdf (last visited Sept. 6, 2016).

> and security incident event management to detect patient privacy breaches, monitor for malicious activities and produce real-time analysis of security alerts
> • 84 percent conduct a third-party security audit annually to ensure that guidelines are followed.[8]

23. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the United States Department of Health and Human Services create rules to streamline the standards for handling Protected Health Information, like the data maintained on Mercy's website.

24. These regulations state that "[a] covered entity or business associate must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information of a covered entity."[9]

25. Despite making the above promises, Mercy did not keep patient's private medical information secure and confidential.

II. Plaintiff's Complaint Revealed That Mercy Failed To Properly Protect Patients' Private Medical Information.

26. Although Mercy represents that it is committed to maintaining patient privacy, Plaintiff's original complaint revealed that Mercy failed to protect the confidential medical information in its care by exposing the private medical information of hundreds of thousands of patients on its websites for months, if not years. Specifically, Mercy's network connected patient medical information portals (e.g., WebStation) lacked basic and fundamental security safeguards and were vulnerable to hacks and further disclosure of confidential medical information.

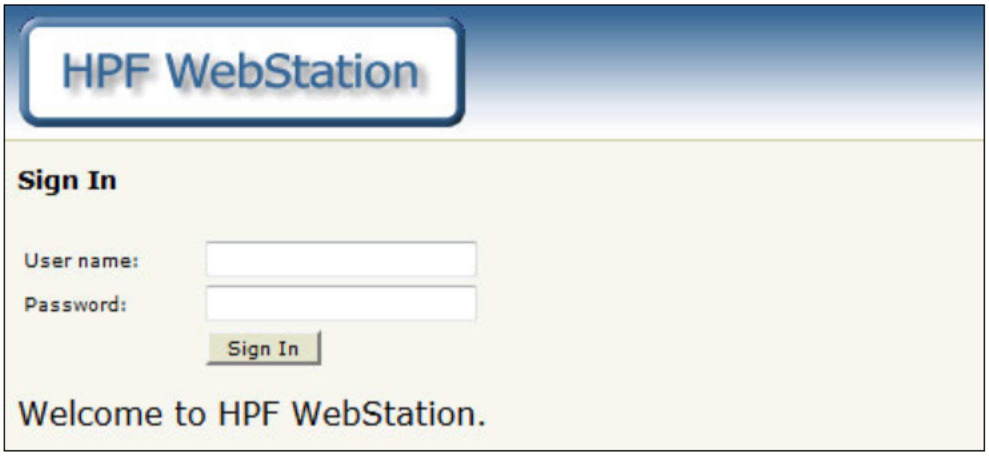
A. Mercy's WebStation Stores Patients' Private Medical Information.

27. Through its WebStation, Mercy allows its employees and agents to access

[8] *Mercy Health a 2016 Most Wired Healthcare System*, http://www.mercy.com/corporate/pdfs/news_releases/2016/Publication_names_Mercy_Health_to_Most_Wired_07_06_16.pdf (last visited Sept. 6, 2016).

[9] 45 C.F.R. § 164.302.

patients' medical information. Defendant Mercy owns and operates the websites 168-250-52-64.health-partners.org, 168-250-52-65.health-partners.org, and 168-250-52-66.health-partners.org where it provides access to its WebStation. Defendant's employees seeking access to patient medical records can use an internet browser (i.e., Google Chrome or Mozilla Firefox) to navigate to a WebStation addresses (e.g., 168-250-52-64.health-partners.org). Once at that website, Defendant's servers load a login prompt where employees are required to enter their usernames and passwords to proceed. *See* Figure 2.



Welcome to HPF WebStation.

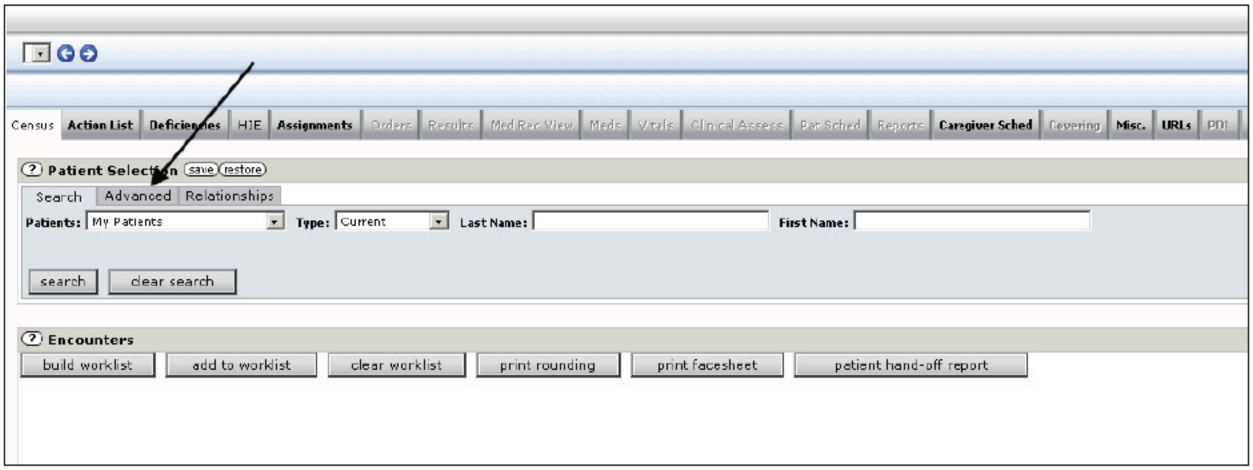
(**Figure 2.**)

28. While Mercy's servers will cause the screen in Figure 2 to appear, behind the scenes, Mercy caused its servers to disclose additional information to visitors. Specifically, Mercy's servers disclose that it uses the "Apache-Coyote/1.1" server and are "Powered-By" "Servlet 2.5; JBoss-5.0/JBossWeb-21."[10]

29. Upon entering a valid username and password, Defendant's systems will present the authorized employee or agent with a screen similar to the one shown in Figure 3. There, the

[10] The information disclosed by Mercy is through the use of optional "HTTP header fields." *HTTP/1.1: HTTP Message*, https://www.w3.org/Protocols/rfc2616/rfc2616-sec4.html (last visited Sept. 6, 2016). Notably, only a server operator (e.g., Mercy) has control over the information disclosed in the HTTP header information—the user simply receives whatever the operator sends. *See id.*

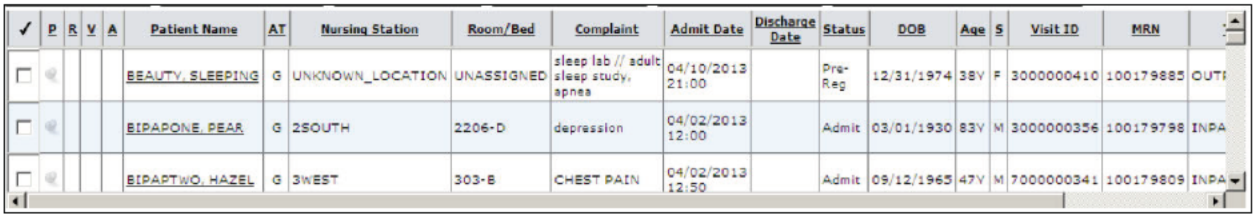
user is able to conduct searches of patients' sensitive medical information, amongst other things.



Patients: My Patients Type: Current Last Name: First Name:

(**Figure 3.**)[11]

30. For instance, the health information contained in Defendant's WebStation service would include each patient's name, admission date, status, date of birth, age, and additional demographic information. *See* Figure 4.



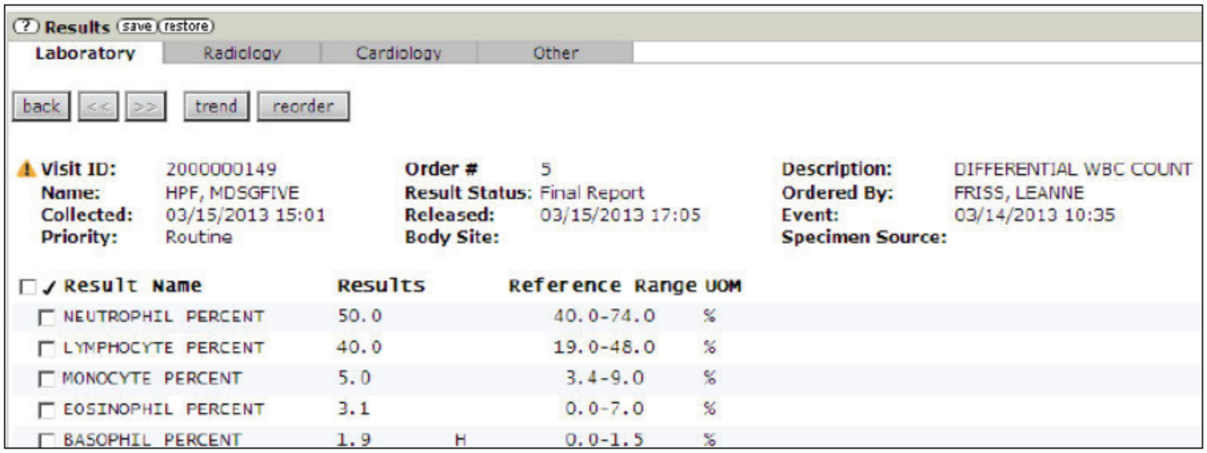
✓	P	R	V	A	Patient Name	AT	Nursing Station	Room/Bed	Complaint	Admit Date	Discharge Date	Status	DOB	Age	S	Visit ID	MRN	
□					BEAUTY, SLEEPING	G	UNKNOWN_LOCATION	UNASSIGNED	sleep lab // adult sleep study, apnea	04/10/2013 21:00		Pre-Reg	12/31/1974	38Y	F	3000000410	100179885	OUTI
□					BIPAPONE, PEAR	G	2SOUTH	2206-D	depression	04/02/2013 12:00		Admit	03/01/1930	83Y	M	3000000356	100179798	INPA
□					BIPAPTWO, HAZEL	G	3WEST	303-B	CHEST PAIN	04/02/2013 12:50		Admit	09/12/1965	47Y	M	7000000341	100179809	INPA

(**Figure 4**, showing sample WebStation data.)[12]

31. The WebStation also stores detailed medical records, such as a patient's diagnosis, treatment, and even specific laboratory results:

[11] HealthAlliance of Hudson Valley, *PHYSICIAN Instructions: Paragon's WebStation for Physicians*, 1, available at http://home.hahv.org/Access/MedicalStaff/Physician/Doctor%20instructions%20Webstation%20for%20physicians.pdf.

[12] *Id.* at 2.



Visit ID:	2000000149	Order #	5	Description:	DIFFERENTIAL WBC COUNT
Name:	HPF, MDSGFIVE	Result Status:	Final Report	Ordered By:	FRISS, LEANNE
Collected:	03/15/2013 15:01	Released:	03/15/2013 17:05	Event:	03/14/2013 10:35
Priority:	Routine	Body Site:		Specimen Source:	

□ ✓ Result Name	Results		Reference Range	UOM
□ NEUTROPHIL PERCENT	50.0		40.0-74.0	%
□ LYMPHOCYTE PERCENT	40.0		19.0-48.0	%
□ MONOCYTE PERCENT	5.0		3.4-9.0	%
□ EOSINOPHIL PERCENT	3.1		0.0-7.0	%
□ BASOPHIL PERCENT	1.9	H	0.0-1.5	%

(**<u>Figure 5</u>**, showing sample laboratory results for fictional "Leanne Friss.")[13]

32. Until several days after the filing of Plaintiff's original Complaint, Defendant's WebStation did not limit access to individuals with valid usernames and passwords. Instead, Defendant left its systems vulnerable to hackers by improperly configuring its services and running out-of-date software. A review of the publically available specifications of Defendant's WebStation service showed that it was built on decade-old software and had not been updated with critical security patches.

B. *Mercy exposed patients' private medical information through its WebStation.*

33. Defendant's WebStation patient information portal is built on a "JBoss Application Server" which implements Java (a virtual computing language) for applications. By using Java, service providers are able to let users run applications on myriad devices without having to rewrite the application for each type device (*e.g.*, a Java application can run on a Mac and a PC without modification).

34. Mercy's implementation of JBoss was woefully out-of-date and suffered from a critical vulnerability (the "JBoss Vulnerability"). As described above, Defendant publicly disclosed that its JBoss system was running version 5.0. A review of industry literature reveals

[13] *Id.* at 5.

that that version of JBoss was introduced in 2008 and is nearing “End of Life” and, as such, is no longer supported or recommended for use. For comparison, the latest version of JBoss (now called WildFly) is version 10.

35. As early as September 2013, the National Institute of Standards and Technology, sponsored by the Department of Homeland Security, updated its National Vulnerability Database to include a vulnerability specific to this version of JBoss. NIST reported that the vulnerability was “network exploitable,” had a “low” level of access complexity, and that it “[a]llows unauthorized disclosure of information; [a]llows unauthorized modification; [and a]llows disruption of service.”[14] Unfixed, JBoss version 5.0 allows hackers to access previously protected information with little to no effort.[15]

36. The risk of this vulnerability is not just theoretical. Computer security experts have recently observed an ongoing and “widespread campaign” attacking JBoss computer systems of the exact type used by Defendant.[16] In these attacks, “[a]dversaries are exploiting known vulnerabilities in unpatched JBoss servers [just like Defendant’s previously unpatched servers] before installing [malicious software], identifying further network connected systems, and installing SamSam ransomware to encrypt files on these devices.” That is, hackers are targeting entities that have not updated their JBoss servers and then holding sensitive data hostage until a ransom is paid.

[14] *NVD – Detail*, https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-4810 (last visited Sep. 6, 2016); *Does CVE-2013-4810 affect Red Hat JBoss products? - Red Hat Customer Portal*, https://access.redhat.com/articles/545183 (last visited Sept. 6, 2016).

[15] Specifically, Mercy’s JBoss implementation has been misconfigured in a way that users can access the “JMXInvokerServlet” and “EJBInvokerServlet” JBoss “servlets” (i.e., server interfaces) without authorization.

[16] *Cisco Talos Blog: SamSam: The Doctor Will See You, After He Pays The Ransom*, http://blog.talosintel.com/2016/03/samsam-ransomware.html?m=1 (last visited Sep. 6, 2016).

37. In one example, a user commented on April 4, 2016 about an attack:

> We were hit by this ransomware and I wasn't sure if it was jboss related or a compromised user account. Good to at least know it was jboss related. We had port 443 open to the world on an aging server[17]

That user, just like Mercy, ran an outdated server that was exposed to the internet ("port 443 open to the world") and was attacked.

38. Earlier this year, the technical publication Ars Technica also reported on the exploitation of the JBoss vulnerability:

> … a number of health providers have been infected recently through Web servers running JBoss.
>
> …
>
> The malware, called "Samsam" by Talos, uses old, very public exploits right out of JexBoss—an open source vulnerability testing tool for JBoss. Once the malware has a foothold on the server, it spreads to Windows machines on the same network.
>
> ….
>
> Of the "couple of dozen targets" … a significant number of them are healthcare organizations. This is likely not because the attackers set out to target healthcare specifically, but because of the types of applications used by hospitals and healthcare networks. Wilson believes that the ransomware developer simply scanned for vulnerable servers on the Internet, and most of the ones that were discovered were at healthcare organizations.
>
> "A lot of people in the healthcare industry—they set up websites in a kind of fire and forget fashion," Wilson explained. "They hire an IT guy, they get the billing system set up, hook it up to the website and then they never touch it again. That's the perfect environment for this type of malware to thrive in because it's not maintained. They have no full-time security staff and few if any fulltime administrators. As a result, the software just goes unpatched."[18]

[17] *Id.*

[18] *Two more healthcare networks caught up in outbreak of hospital ransomware | Ars Technica*, http://arstechnica.com/security/2016/03/two-more-healthcare-networks-caught-up-in-outbreak-of-hospital-ransomware/ (last visited Sept. 6, 2016).

39. As Ars Technica stated, vulnerabilities like the one Mercy had on its WebStation often serve as the entry point to other sensitive and potentially vulnerable systems. Mercy undoubtedly has a host of network connected medical devices in its hospital systems that may be vulnerable to hackers, including MRI machines[19], drug infusion machines[20], and robotic surgical equipment[21]. Each of those systems might suffer from their own vulnerabilities (or may not be protected by any mechanism at all) and if a hacker gains access to them, he or should could tamper with at-risk patients and the delivery of vital medical care.

40. For instance, a service related to the WebStation service also has a vulnerability that, in this case, *cannot* be remedied. According to a service that tracks security vulnerabilities, "The McKesson Horizon Clinical Infrastructure (HCI) software uses common, hardcoded passwords for the Oracle database. A remote user with knowledge of the passwords can connect to the target database."[22] That is, every instance of McKesson's HCI software (e.g., installed in different hospitals across the country) uses the *same* password and entities cannot change that password. If a hacker gained access through Mercy's JBoss Vulnerability, there are few (if any) additional security measures to protect against further unauthorized access and disclosure of

[19] *Medical devices could be lethal in hands of hackers | TheHill*, http://thehill.com/policy/cybersecurity/271003-medical-devices-could-be-lethal-in-hands-of-hackers (last visited Sept. 6, 2016) (stating that "Hackers could disable a certain commonly used piece of equipment, like an MRI machine, effectively withholding needed care.")

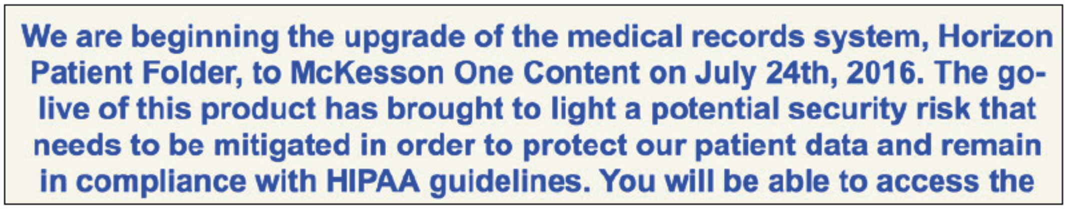
[20] *Medical Devices That Are Vulnerable to Life-Threatening Hacks | WIRED*, https://www.wired.com/2015/11/medical-devices-that-are-vulnerable-to-life-threatening-hacks/#slide-1 (last visited Sept. 6, 2016) (noting that researchers "found vulnerabilities in the pump that would allow a hacker to surreptitiously and remotely change the amount of drugs administered to patients to deliver a deadly dosage.")

[21] *Telesurgery Vulnerable to Remote Hacks, Hijacks*, https://blog.kaspersky.com/hacking-robotic-surgeons/8570/ (last visited Sept. 6, 2016) (stating that "A group of academic security researchers remotely hacked and took control of a robot designed to perform telesurgery.")

[22] *McKesson Horizon Products Use Hardcoded Database Passwords That May Allow Remote Users to Access the System – SecurityTracker*, http://securitytracker.com/id/1023050 (last visited Sept. 6, 2016).

highly sensitive patient medical information. And, although Mercy fixed the JBoss Vulnerability, it does not guarantee that Mercy's systems had not already been breached.

41. Making matters worse, Mercy was likely notified by McKesson (or others) *prior* to the filing of Plaintiff's original complaint that the WebStation was vulnerable and should not have been used to store patients' private medical information. Lovelace Hospital system of New Mexico also utilizes the WebStation system from McKesson and issued the following notice on its webpage:



We are beginning the upgrade of the medical records system, Horizon Patient Folder, to McKesson One Content on July 24th, 2016. The go-live of this product has brought to light a potential security risk that needs to be mitigated in order to protect our patient data and remain in compliance with HIPAA guidelines. You will be able to access the

(**<u>Figure 6</u>**.)[23]

42. There, just as here, Lovelace Hospital System ran the Horizon Patient Folder built by McKesson. And, Lovelace's HPF—just like Mercy's—suffered from a "potential security risk" that while unfixed resulted in Lovelace not being "in compliance with HIPAA guidelines."

43. Plaintiff filed his initial Complaint on August 2, 2016, alerting Mercy of the JBoss Vulnerability. In his Complaint and in the Expert Report of Craig J. Snead Plaintiff laid out the severity of the JBoss Vulnerability, how Mercy was exposing patient data to theft, and that a breach was imminent unless the vulnerability was fixed (if Mercy wasn't already breached). Then, on August 5, 2016—just three days after Plaintiff filed his complaint—Defendant fixed the JBoss Vulnerability.

44. Despite this fix—which, as Plaintiff's expert explains, could have been done

[23] A true and accurate screenshot of the webpage *HorizonWP Physician Portal*, https://myportal.lovelace.com/portal/site/nonss/ as it appeared on July 18, 2016 is attached hereto as Exhibit C.

"quickly and cheaply" at any time[24]—Mercy still exposed patient data for months, if not years. Given the nature of the vulnerability (which was easily exploitable), there is a high likelihood that Mercy's patient data had already been compromised and, thus, Plaintiff and other Class Members will continue to face the risk of additional, imminent harm far into the future (i.e., until such time that third parties can verify that—despite Mercy's conduct—Plaintiff and Class Members' patient data was not accessed without authorization during the relevant time period).

C. Mercy ignored industry standards, leaving patients' private medical information exposed.

45. Consumer expectations, HIPAA, and State law requires that healthcare providers (like Mercy) adopt industry standard administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of consumers' confidential medical information. If Mercy followed industry standards, patients' private medical information would not have been exposed and/or compromised. Indeed, industry standard practices (and common sense) dictate that only verified Mercy employees or agents (e.g., physicians and medical personnel) should have been granted access to patients' private medical information and that all others should be prohibited from accessing that information. Myriad methods exist to ensure that does not happen on even the most basic of websites and services. For websites that maintain sensitive information, such as medical records, there exist governmental organizations, industry groups, and others that recognize the heightened demand for security and, as such, outline protocols to ensure data integrity.

46. Broadly speaking, Mercy's security failures demonstrate that it failed to implement industry standard user verification techniques and data security as required by

[24] Snead Decl. at ¶ 16.

consumer expectations, federal and state law, and its contract with patients. More specifically, Mercy:

a. Failed to maintain an adequate data security system to prevent data breaches;

b. Failed to mitigate the risks of a data breach and unauthorized access to protected health information;

c. Failed to encrypt or otherwise protect Plaintiff's and the Class's protected health information;

d. Failed to ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1);

e. Failed to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failed to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failed to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. § 164.306(a)(2);

h. Failed to protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

i. Failed to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4);

j. Failed to effectively train all members of its workforce on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R § 164.530(b);

k. Failed to design, implement, and enforce policies and procedures establishing administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. § 164.530(c);

l. Failed to protect the privacy of patients as promised in Mercy's Notice of Privacy Practices;

m. Failed to create and maintain records of patients that meet legal requirements as promised in Mercy's Notice of Privacy Practices;

n. Failed to follow the terms of the notice as promised in Mercy's Notice of Privacy Practices; and,

o. Failed to notify patients that Mercy failed to protect their privacy as promised in Mercy's Notice of Privacy Practices.

47. Mercy also failed to comply with industry standards. Over a decade ago, in March 2005, the National Institute of Standards and Technology ("NIST") published a report detailing standards for healthcare providers seeking to comply with HIPAA's Security Rule. In the report, NIST recommended specific techniques to safeguard electronically stored sensitive information. In one example, NIST specifically recommended that companies use "authentication mechanisms [] to verify the identity of those accessing systems protected from inappropriate manipulation."[26]

48. In addition, the United States Department of Health and Human Services ("HHS") has issued many documents to assist covered entities better secure patient data. In a white paper on "Security Standards: Technical Safeguards," the HHS explains that:

> In general, authentication ensures that a person is in fact who he or she claims to be before being allowed access to [electronic protected health information ("EPHI")]. This is accomplished by providing proof of identity. There are a few basic ways to provide proof of identity for authentication. A covered entity may:
>
> - Require something known only to that individual, such as a password or PIN.
>
> - Require something that individuals possess, such as a smart card, a token, or a key.

[26] Matthew School et al., National Institute of Standards and Technology, U.S. Dep't of Commerce, *NIST Special Publication 800-66 Revision 1: An Introductory Resources Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule* (Oct. 2008), at 23, *available at* http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf.

> - o Require something unique to the individual such as a biometric. Examples of biometrics include fingerprints, voice patterns, facial patterns or iris patterns.
>
> Most covered entities use one of the first two methods of authentication. Many small provider offices rely on a password or PIN to authenticate the user. If the authentication credentials entered into an information system match those stored in that system, the user is authenticated. Once properly authenticated, the user is granted the authorized access privileges to perform functions and access EPHI.[27]

49. Mercy ignored many other long-standing industry protocols, including the standard practice of regular auditing and monitoring of systems that protect sensitive information. In 1996, NIST issued the "Principles and Practices for Security IT Systems," and while many specific technologies have changed since that document's release, the underlying guidelines have stayed the same.[28] For instance, once a system has been deployed, organizations are to conduct "[a] system audit [which] is a one-time or periodic event to evaluate security" and to "monitor[] … ongoing activity [to] examine[] either the system or the users."[29] One audit specifically mentioned (and used more commonly in the industry today) is "Penetration Testing," which is described as follows:

> Penetration testing can use many methods to attempt a system break-in. In addition to using active automated tools as described above, penetration testing can be done "manually." For many systems, lax procedures or a lack of internal controls on applications are common vulnerabilities that penetration testing can target. Penetration testing is a very powerful technique; it should preferably be conducted with the knowledge and consent of system management.[30]

50. If Mercy conducted even a basic penetration test to look for cyber security

[27] Department of Health and Human Services, *HIPAA,* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf (last visited Sept. 6, 2016).

[28] U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, *Generally Accepted Principles and Practices for Security Information Technology Systems*, 24 (available at http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf).

[29] *Id.*

[30] *Id.* at 25.

weaknesses, it would have uncovered the JBoss Vulnerability and could have remedied it immediately. The nature of the JBoss Vulnerability (i.e., that it is caused by a misconfigured file) suggests that Mercy's system has been vulnerable since it first implemented WebStation, many years ago. Had Mercy conducted any credible penetration testing over that time, it would have been alerted that its systems are vulnerable—*especially* given that the specific JBoss vulnerability had been warned of since at least 2013—and it would have fixed the issue immediately.

51. Mercy's actions are alarming. Mercy patients both expect and paid for (as a part of their medical payments) the confidentiality of their private medical information as part of receiving and paying for medical treatment, but Mercy exposed that information. Moreover, Mercy profited by not allocating necessary resources to keep that information confidential (*e.g.*, by implementing industry standard information security). And while Mercy has taken recent steps to secure the patient data in its control—only after a patient took it to task for failing to do so—that does not excuse Mercy's long-standing policy of ignoring plain security risks and, for years, exposing its patients' confidential information.

III. Patient Medical Information is a Primary Target for Hackers.

52. Patients were not only injured by Mercy's failure to provide the security they paid for, but because Mercy exposed their information for months (if not years), they run the risk of being victims of further harm, including identity theft and physical harm from altered medical records.

53. This risk is (and was) especially great for Mercy's patients, considering the sensitive type of information with which they entrusted to Mercy. While companies of all sizes are increasingly at risk of having sensitive information stolen, the risk is exacerbated in the

medical industry as patients' private medical records become digitized. Identity thieves have specifically targeted private medical information because that data is more valuable than other types, such as even credit card numbers. As a result, medical organizations and companies that provide services to those organizations have been specifically warned to strengthen security measures.

54. In a June 2007 report on data theft, the United States Government Accountability Office noted that identity thieves use stolen information to open financial accounts, receive government benefits, and incur charges and open credit in a person's name.[31] As the report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft, which can adversely impact the victim's credit rating. Victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[32]

55. Worse, a person whose personal information has been compromised may not see any signs of identity theft for years:

> "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[33]

56. Stolen medical information is a valuable commodity to identity thieves who often trade the information on cyber black-markets. Indeed, entire online "underground exchanges" have been created "where hackers sell [stolen] information," such as "names, birth dates, policy

[31] *See* United States Government Accountability Office, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), *available at* www.gao.gov/new.items/d07737.pdf.

[32] *Id.*

[33] *Id.*

numbers, diagnosis codes and billing information."[34] On these exchanges, "medical information is worth 10 times more than [] credit card number[s]."[35] One report noted that "[h]ealth insurance credentials are especially valuable in today's economy because health care costs are causing people to seek free medical care with these credentials."[36]

57. Examples of medical data breaches are legion. The U.S. Department of Health and Human Services Office for Civil Rights maintains an up-to-date list of every reported "breach[] of unsecured protected health information affecting 500 or more individuals."[37] At last count, there were over 1,600 reported incidents since October 2009—more than one breach every other day.[38] In one recent case, a "niche pharmaceutical company" suffered a breach of "50,000 records" and was being held ransom by a "hacker who [was looking] to sell the data to the highest bidder or back to the company, whichever comes first."[39]

58. In another example from September of 2015, Systema Software, a company that works with physicians and clinics to provide access to patients' medical information over the internet (not unlike Mercy), improperly secured the private medical information of approximately 1.5 *million* patients.[40] There, Systema Software apparently failed to implement

[34] *Your medical record is worth more to hackers than your credit card | Reuters*, www.reuters.com/article/ 2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924 (last visited Sept. 6, 2016).

[35] *Id.*

[36] *Why hackers want your health care data most of all | InfoWorld*, www.infoworld.com/article/2983634/ security/why-hackers-want-your-health-care-data-breaches-most-of-all.html (last visited Sept. 6, 2016).

[37] *U.S. Department of Health & Human Services - Office for Civil Rights*, ocrportal.hhs.gov/ocr/breach/ breach_report.jsf (last visited Sept. 6, 2016).

[38] *Id.*

[39] *Akorn Inc. has customer database stolen, records offered to highest bidder | CSO Online*, www.csoonline. com/article/2938032/data-breach/akorn-inc-has-customer-database-stolen-records-offered-to-highest-bidder.html (last visited Sept. 6, 2016).

[40] *Oops! Error by Systema Software exposes millions of records with insurance claims data and internal notes (Update2)*, http://www.databreaches.net/oops-error-by-systema-software-exposes-millions-of-records-with-insurance-claims-data-and-internal-notes/ (last visited Sept. 6, 2016).

industry-standard authentication protocols, allowing a "self-described 'technology enthusiast'" to breach its systems to access and download patients' "name, Social Security Number, phone number, address," "financial transaction data," and "insurance claim forms with some medical/health information." Had Systema Software implemented basic security features, the breach would have been thwarted. As it stands, the company joins the growing list of companies that have been breached.

59. In fact, the American Bar Association published a book warning companies that store patient data that "[m]assive data breaches are occurring with alarming frequency. An analysis of data breaches by industry should provide a wake-up call for the health care industry."[41] The ABA went on, saying that "[f]ailed security has resulted in massive data breaches that led to the loss or compromise of millions of personally identifiable health care records. … In almost all cases, data breaches that occurred could have been prevented by proper planning and the correct security design and implementation of appropriate security safeguards."[42]

60. As such, companies entrusted with sensitive patient medical information must be vigilant against threats and employ (at a bare-minimum) industry-standard cyber protection. Any cost borne by the company to implement those practices is dwarfed by the cost faced by consumers who are victim to a medical data breach. The "average total cost" of medical identity theft is "about $20,000" per incident, according to a report by Experian, and the majority of victims of medical identity theft are forced to pay out-of-pocket costs for health care they did not receive (*i.e.*, fraudulent medical billing and services) just to restore medical or insurance

[41] *Health Care Data Breaches and Information Security*, www.americanbar.org/content/dam/aba/publications/books/healthcare_data_breaches.authcheckdam.pdf (last visited Sept. 6, 2016).

[42] *Id.*

coverage.[43] Indeed, almost half of medical identity theft victims lose their health care coverage as a result of such incidents, nearly one-third will see their insurance premiums rise, and forty percent are likely to never to get closure of their identity theft.[44] Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

61. Importantly, the disclosure and theft of medical data has effects far beyond money costs, including dangerous physical consequences and reputational harm. In 2014, CBS News reported that "[m]edical identity theft can threaten health as well as bank account[s]."[45] The report went on to state that "15 percent of the medical identity theft victims surveyed reported that the theft had created misinformation in their medical records that led to a misdiagnosis, and 14 percent said they experienced a delay in care."[46] Because of this, "[t]he impact of medical identity theft can be even more dire than financial identity theft."[47]

62. And in a February 2015 study, the Ponemon Institute—a group "dedicated to independent research and education that advances responsible information and privacy management practices within business and government"—reported that "medical identity theft affected [victims'] reputation mainly because of embarrassment due to disclosure of sensitive personal health conditions."[48] Ponemon went on to report that the disclosure of that potentially embarrassing personal health information has led victims to "miss out on career opportunities"

[43] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, news.cnet.com/8301-27080_3-10460902-245.html (last visited Sept. 6, 2016).

[44] *Id.*

[45] *Experts say medical identity theft is "low-hanging fruit" for thieves; cite limited police attention and lack of record-keeping - CBS News*, http://www.cbsnews.com/news/medical-identity-theft-can-threaten-health-as-well-as-bank-account/ (last visited Sept. 6, 2016).

[46] *Id.*

[47] *Id.*

[48] Ponemon Institute, *Fifth Annual Study on Medical Identity Theft*, (Feb. 2015) available at http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf

and lose their jobs.[49]

63. And if these warnings against and dire consequences of disclosing sensitive health-related data were not enough, Mercy is specifically on notice that hackers and identity thieves target Ohio patients' private medical information. The same morning Plaintiff filed his Complaint, news broke that hackers breached the second largest Ohio hospital system (only behind Mercy) and stole thousands of patients' detailed medical and payment records.[50] The breach included, amongst other things, "payment info and patients medical data," "complaint/reason history of present illness, active medications, allergies, past medical/surgical history, diagnostics history and family history," and "the entire architecture design of the data center … with absolutely no security whatsoever."[51] As HackRead.com reported:

> The breach of the Central Ohio Urology Group illustrates how healthcare system file collaboration has become the new data leakage frontier," said Scott Gordon, chief operating officer at FinalCode. "Given HIPAA and HITECH legislation, providers need to assume incidents will occur. A proactive stance, invoking available encryption and usage control on files such as the more than 100,000 exposed Microsoft and Adobe documents in the Ohio breach, would have secured this regulated data and enabled breach disclosure safe harbors."[52]

64. Given the recognized targeting of patient data by identity thieves, it is likely that the confidential patient data entrusted to—and posted online with *no* data security protections by—Defendant may have already been compromised and misused. Mercy's websites had been operating for months (or years) with the vulnerabilities described here. And because of poor security management and administration, there is a strong chance that Mercy is ignorant of prior

[49] *Id.*

[50] *Hacker Dumps Sensitive Patient Data From Ohio Urology Clinics | Motherboard*, https://motherboard.vice.com/read/hacker-dumps-sensitive-patient-data-from-ohio-urology-clinics (last visited Sept. 6, 2016).

[51] *Central Ohio Urology Group Hacked; 223GB of Crucial Data Leaked (Updated)*, https://www.hackread.com/central-ohio-urology-group-hacked/ (last visited Sept. 6, 2016).

[52] *Id.*

or continuing unauthorized access or use stemming from the website vulnerabilities. That is, a hacker could have already infiltrated Defendant's systems and planted malware.[53]

65. As such, the only way to further protect Plaintiff's and other similarly situated patients' confidential patient data is to require Defendant to allow an independent third-party firm to conduct a security audit its systems to ensure the integrity of patients' private medical information and determine the extent of any data breach that may have already occurred. Without the assurance of an independent third party auditor who can establish that no breach occurred, Plaintiff and members of the Class cannot be certain that Mercy has not impaired the integrity of their private medical information.

PLAINTIFF WILLIAMS-DIGGINS'S EXPERIENCE

66. Plaintiff Williams-Diggins has been a patient at Mercy affiliated facilities for more than a decade, and has regularly visited a Mercy affiliated clinic in Maumee, Ohio. During that time, Plaintiff received care and Mercy created electronic records of Plaintiff's visits. Plaintiff routinely paid (directly through deductibles and/or copays and indirectly through his insurance premiums) for the medical care he received. During these visits, Mercy provided him with its Notice of Privacy Practices.

67. Plaintiff paid for the medical care he received because he had the reasonable expectation that Mercy was keeping his medical information confidential, formed, in part, from Mercy's Notice of Privacy Practices. Moreover, Plaintiff understood and expected that

[53] *See FBI Says a Mysterious Hacking Group Has Had Access to US Govt Files for Years | Motherboard*, http://motherboard.vice.com/read/fbi-flash-alert-hacking-group-has-had-access-to-us-govt-files-for-years (last visited Sept. 6, 2016) (stating that "The [FBI's] alert … shows that foreign government hackers are still successfully hacking and stealing data from US government's servers, their activities going unnoticed for years.")

companies entrusted with private medical information are required by law (*e.g.*, HIPAA) to use industry standard security protections to safeguard the data and keep it confidential. Plaintiff values the privacy of his private medical information and avoids doing business with companies with lax data security protocols.

68. Plaintiff's private medical information is being maintained on Mercy's servers and was exposed without his authorization.

CLASS ALLEGATIONS

69. **Class Definitions:** Plaintiff brings this class action pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), and (b)(3) on behalf of himself and a Class and Subclass of similarly situated individuals, defined as follows:

> **Class**: All persons in the United States who have received medical care at a Mercy facility and who have their medical information stored electronically by Defendant.
>
> **Ohio Subclass**: All individuals in the Class who are domiciled in the State of Ohio.

The following persons are excluded from the Class and Ohio Subclass ("the Class"): (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and their current or former employees, officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

70. **Numerosity:** On information and belief, tens of thousands of consumers fall into the Class definition. Members of the Class can be identified through Defendant's records.

71. **Commonality and Predominance:** Common questions of law and fact exist as to all members of the Class and, pursuant to Fed. R. Civ. P. 23(b)(3), predominate over any questions affecting only individual members. Those questions with respect to the Class include, but are not limited to:

(a) Whether Mercy exposed its patients' private medical information;

(b) Whether Mercy failed to safeguard patients' private medical information;

(c) Whether Mercy compromised the integrity of patients' private medical information;

(d) Whether Defendant's storage of patients' private medical information in the manner alleged violated HIPAA, federal, state and local laws, or industry standards;

(e) Whether Defendant was obligated to notify Plaintiff and the other members of the Class about the exposed patient information as soon as practical and without delay after it was discovered;

(f) Whether Mercy failed to adequately secure patients' private medical information;

(g) Whether contracts exist between Defendant, on the one hand, and Plaintiff and the other members of the Class, on the other;

(h) Whether Mercy breached its contracts with Plaintiff and the other members of the Class;

(i) Whether Mercy violated the Ohio Consumer Sales Protection Act;

(j) Whether Mercy has been unjustly enriched;

(k) Whether Mercy breached the confidence of Plaintiff and the Ohio

Subclass; and

(l) Whether Plaintiff and the Class are entitled to a permanent injunction to protect and evaluate the integrity of their private medical information.

72. **Typicality**: Plaintiff's claims are typical of the claims of the other members of the Class, in that Plaintiff and the other members of the Class continuously sustain injury arising out of Defendant's wrongful conduct.

73. **Adequate Representation:** Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff's claims are representative of the claims of the other members of the Class. That is, Plaintiff and the other Class members each have their private medical information insecurely stored on Defendant's servers and require an injunction to safeguard their data and have paid for Mercy's services with a portion of each payment to be uses for the administrative costs of data management and security. Plaintiff also has no interests antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the other members of the Class, and have the financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to the Class.

74. **Policies Generally Applicable to the Class**: This class action is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the other members of the Class and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies that Plaintiff challenges apply and affect the members of the Class uniformly and Plaintiff's challenge of these policies

hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff. The factual and legal bases of Defendant's liability to Plaintiff and to the other members of the Class are the same.

75. **Separate Suits Would Create Risk of Varying Conduct Requirements**: The prosecution of separate actions by the members of the Class against Mercy would create a risk of inconsistent or varying adjudications with respect to individual members of the Class that would establish incompatible standards of conduct. Certification is therefore proper under Fed. R. Civ. P. 23(b)(1).

76. **Appropriateness of Injunctive Relief**: Pursuant to Fed. R. Civ. P. 23(b)(2), Defendant has acted on grounds generally applicable to the Class, thereby making final injunctive relief appropriate with respect to the Class as a whole. Prosecution of separate actions by individual members of the Class would create the risk of inconsistent or varying adjudications with respect to individual members of the Class that would establish incompatible standards of conduct for Defendant.

77. **Superiority**: This case is also appropriate for certification, pursuant to Fed. R. Civ. P. 23(b)(3), because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy. The harm suffered by the individual members of the Class is likely to have been relatively small compared to the burden and expense of individual prosecution of litigation to redress Defendant's actions. Absent a class action, it would be difficult if not impossible for the individual members of the Class to obtain effective relief from Defendant. Even if members of the Class members themselves could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties and the Court and require duplicative

consideration of the legal and factual issues presented. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single Court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

78. Plaintiff reserves the right to revise the foregoing "Class Allegations" and "Class Definition" based on facts learned through additional investigation and in discovery.

COUNT I
Breach of Contract
(On behalf of Plaintiff and the Class)

79. Plaintiff incorporates by reference the foregoing allegations as if fully set forth herein.

80. Plaintiff and the other Class members entered into contracts with Defendant to receive medical care. The terms of the contracts include or incorporate by reference the promises and representations found in Defendant's Notice of Privacy Practices, as described in Section I. *See* Exhibit A.

81. Mercy provides the Notice of Privacy Practices to each patient and requires each patient to state in writing that they received the Notice of Privacy Practices.

82. As detailed in this Complaint, Defendant breached its patient contracts by failing to protect Plaintiff's and the other Class members' private medical information. As described above, Defendant exposed Plaintiff's and the other Class members' private medical information for months or years through, at least, its websites that suffered from the JBoss Vulnerability.

83. Moreover, Defendant breached its patient contracts by failing to institute industry standard measures, and measures required by federal and state law (as promised) to protect Plaintiff's and the other Class members' private medical information.

84. At all times relevant to this action, Defendant acted willfully and with intent to breach contracts entered into with Plaintiff and the Class. Specifically, Mercy (and its website developers and network security employees) programmed its websites and designed and configured them with inadequate safeguards.

85. Plaintiff and the other Class members have fully performed their contractual obligations by paying (directly or indirectly) for the services they received and providing Mercy with their private medical information.

86. As a direct and proximate result of Defendant's breach, Plaintiff and the other Class members have suffered—and, through this action, seek to recover—damages in an amount equal to the difference in the value of the secure healthcare services they paid for and the insecure healthcare services Mercy provided. Specifically, Plaintiff and the other Class members have been injured by receiving healthcare services that were of less value than they paid for (i.e., healthcare services without adequate data security and management practices). Stated otherwise, Plaintiff and the other members of the Class did not receive the full benefit of their bargain because they paid for privacy protections (as part of, among other things, their co-pays and medical bills, and indirectly through their insurance premiums and deductibles), which are material parts of their contracts with Defendant, but Defendant failed to implement (or partially or defectively implemented) such protections, despite its promise and obligation to do so.

COUNT II
Unjust Enrichment
(In the alternative to Count I)
(On behalf of Plaintiff and the Class)

87. Plaintiff incorporates by reference the foregoing allegations as if fully set forth herein.

88. Plaintiff hereby pleads Count II in the alternative to Count I.

89. Plaintiff and members of the Class conferred a measurable monetary benefit on Defendant. Defendant received and retained money belonging to Plaintiff and the Class in the form of a portion of the medical fees paid to Mercy.

90. Defendant appreciates or has knowledge of such benefit.

91. A portion of the medical fees that Plaintiff and the Class paid to Defendant was to be used by Mercy, in part, to pay for the administrative costs of data management and security (*i.e.*, to keep their private medical information confidential and protected).

92. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and members of the Class. Defendant has failed to keep Plaintiff's and Class members' private medical information confidential and failed to implement industry standard data management and security measures to secure patients' private medical information, and under such circumstances, Defendant's retention of the benefit without payment would be unjust.

93. Accordingly, Mercy has received money from Plaintiff and the Class through the unlawful practices alleged herein, which in equity and good conscience should be returned.

COUNT III
Breach of Confidence
(On behalf of Plaintiff and the Ohio Subclass)

94. Plaintiff incorporates by reference the foregoing allegations as if fully set forth herein.

95. Plaintiff and members of the Ohio Subclass are residents of the State of Ohio.

96. In leaving its WebStation systems vulnerable, Defendant made unauthorized and unprivileged disclosures to third parties of nonpublic medical information that a physician or hospital has learned within a physician-patient relationship.

97. Plaintiff's and Ohio Subclass members' private medical information stored on Defendant's WebStation system is nonpublic medical information. Defendant learned of that information through a physician-patient relationship.

98. Plaintiff and members of the Ohio Subclass did not and have not provided consent to Defendant to disclose their nonpublic medical information to any third party in the way described herein.

99. Defendant's WebStation system had the JBoss Vulnerability, which was publicly disclosed in 2013, for months if not years. Since the JBoss Vulnerability has been publicly disclosed, Defendant did not update or patch its systems to protect against it until three days after Plaintiff filed his original complaint. As such, Defendant acted intentionally by failing to mitigate the JBoss Vulnerability and by exposing Plaintiff's and Ohio Subclass members' nonpublic medical information.

100. Plaintiff, on his own behalf and on behalf of the Ohio Subclass, seeks restitution, damages resulting from Defendant's breach of confidence, and to recover the costs of suit, including reasonable attorneys' fees.

COUNT IV
Violations of the Ohio Consumer Sales Protection Act
Ohio Rev. Code § 1345.09(D)
(On behalf of Plaintiff and the Ohio Subclass)

101. Plaintiff incorporates by reference the foregoing allegations as if fully set forth herein.

102. The Ohio Consumer Sales Protection Act (the "Ohio CSPA") prohibits suppliers from using "unfair or deceptive act or practice in connection with a consumer transaction" that occur "before, during, or after the transaction."

103. Defendant, Plaintiff, and each member of the Ohio Subclass is a "Person" as

defined by Ohio Rev. Code § 1345.01(B) because they are each an individual or a corporation, government, governmental subdivision or agency, business trust, estate, trust, partnership, association, cooperative, or other legal entity.

104. Defendant is a "Supplier" as defined by Ohio Rev. Code §1345.01(C) because it is a seller or other person engaged in the business of effecting or soliciting consumer transactions, whether or not the person deals directly with the consumer.

105. Plaintiff and each member of the Ohio Subclass entered in to a "Consumer Transaction" as defined by Ohio Rev. Code §1345.01(A) because they purchased goods and services from Defendant for primarily personal, family, or household use. The consumer transactions do not include transactions between Plaintiff and members of the Ohio Subclass and any physicians because Defendant is not a physician.

106. Plaintiff and each member of the Ohio Subclass is a consumer as defined by Ohio Rev. Code § 1345.01(D) because they are each a person who engaged in a consumer transaction with Defendant, a supplier.

107. Defendant violated the CSPA because it failed to implement basic security protocols, thereby exposing Plaintiff's and the Ohio Subclass's private medical information and placing that information at risk of further unauthorized disclosure. Defendant's actions were unfair because Mercy makes representations to consumers that it will keep their private medical information secure, Mercy receives payments (by and through Plaintiff and the Ohio Subclass paying their medical bills) to keep that information secure, and Mercy is obligated under federal and state law to employ safeguards to secure the private medical information.

108. Specifically, Defendant's actions violated the Ohio CSPA in at least the following respects:

a. Violating 1345.02(B)(1) by representing that its medical services have sponsorship, approval, performance characteristics, accessories, uses, or benefits that they does not have; and

b. Violating 1345.02(B)(2) by representing that its medical services are of a particular standard, quality, grade, style, prescription, or model, even when they are not.

109. In the course of its consumer transactions, Defendant exposed the private medical records of tens of thousands of Ohio residents. Moreover, Mercy continuously maintains and ventures to obtain additional private medical information from the public in the State of Ohio, yet failed to adequately protect the public's private medical information for months if not years, which put tens of thousands of Ohio residents at risk of having their information further disclosed without authorization.

110. Plaintiff and members of the Ohio Subclass paid Mercy medical fees for medical treatment, and Mercy received and has knowledge of that payment. The medical fees that Plaintiff and the Ohio Subclass (directly or indirectly) paid to Mercy are (or should have been) used by Mercy, in part, to pay for the administrative costs of data management and security. However, Plaintiff and the Ohio Subclass did not receive the full benefit of their transactions and Mercy unfairly profited (and likely still profits) by not providing the paid-for services. Stated otherwise, because of Mercy's conduct, Plaintiff and members of the Ohio Subclass did not receive the full benefit of their bargains and, instead, received health care services that were less valuable than those Mercy promised. Plaintiff and Ohio Subclass members therefore were damaged in an amount at least equal to the difference in value between that which was promised and the health care services that Mercy provided.

111. As a direct and proximate result of Defendant's unfair and/or deceptive conduct, Plaintiff and members of the Ohio Subclass have suffered injury because Mercy exposed their private medical information on its websites; they have suffered a diminished value of the Mercy services they received.

112. Accordingly, Plaintiff and the Ohio Subclass seek actual damages, injunctive relief, and the costs of suit, including reasonable attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Lindsey Williams-Diggins, on behalf of himself and members of the Class, prays for the following relief:

a. An order certifying this case as a class action on behalf of the Class and Subclass defined above, appointing Lindsey Williams-Diggins as representative of the Class and Subclass, and appointing his counsel as class counsel; and,

b. An order:

i. Declaring that Defendant's conduct, as set out above, constitutes a breach of contract, unjust enrichment, breach of confidence, and a violation of the Ohio CSPA;

ii. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including an order (i) prohibiting Mercy from engaging in the wrongful and unlawful acts described herein; (ii) requiring Mercy to protect all data collected through the course of its business in accordance with its own representations, HIPAA regulations, federal, state and local laws, and industry standards; (iii) requiring Mercy to engage third-party forensic security professionals as well as internal security personnel to conduct analysis of relevant logs and records to determine whether Mercy's systems have already been breached or if Mercy's exposure of patients' private medical information through the JBoss Vulnerability constitutes a data breach; and (iv) requiring Mercy to promptly notify members of the Class if it is determined that Mercy has already been breached or the JBoss Vulnerability constitutes a breach.

iii. Awarding actual damages to Plaintiff and the Class, where applicable, in an amount to be determined at trial;

iv. Awarding restitution to Plaintiff and the Class in an amount to be determined at trial;

v. Awarding reasonable attorney's fees and expenses;

vi. Awarding pre- and post-judgment interest, to the extent allowable; and,

vii. Award such other and further relief as equity and justice may require.

JURY DEMAND

Plaintiff requests trial by jury of all claims that can be so tried.

Respectfully Submitted,

LINDSEY WILLIAMS-DIGGINS, individually
and on behalf of all others similarly situated,

Dated: September 6, 2016

By: ______________________
One of Plaintiff's Attorneys

Cathleen M. Bolek (0059884)
Bolek Besser Glesius, LLC
Monarch Centre, Suite 302
5885 Landerbrook Drive
Cleveland, Ohio 44124
Tel: 216.464.3004
Fax: 866.542.0743
cbolek@bolekbesser.com

Rafey S. Balabanian (*pro hac vice*)
rbalabanian@edelson.com
Eve-Lynn J. Rapp (*pro hac vice*)
erapp@edelson.com
EDELSON PC
123 Townsend Street
San Francisco, California 94107
Tel: 415.212.9300
Fax: 415.373.9435

Benjamin S. Thomassen (*pro hac vice*)
bthomassen@edelson.com
EDELSON PC
350 North LaSalle Street, 13th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378